

How to Configure the Legacy Barracuda Web Security Service aka FLEX

<https://campus.barracuda.com/doc/53248823/>

This article is for the legacy Barracuda Web Security Service, formerly known as FLEX. To configure the new Barracuda Web Security Service, see [How to Configure Web Security Service Integration using GRE Tunnels and a Static Public IP](#).

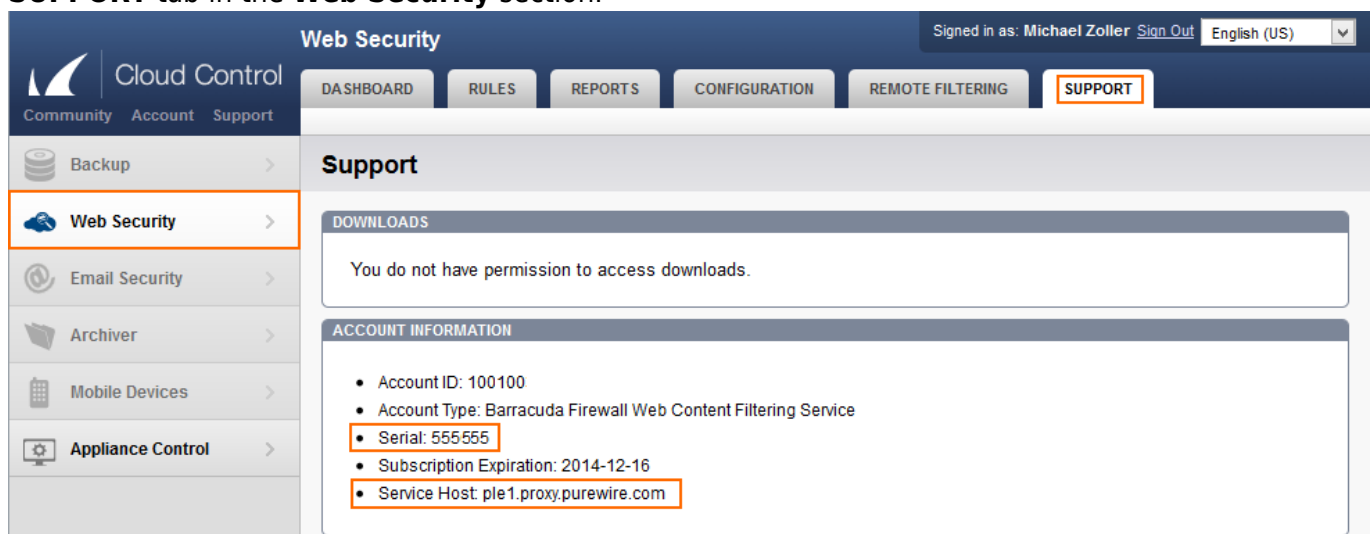
To apply central usage policies and scan your web traffic for malware or unwanted content, forward web traffic to the Barracuda Web Security service, formerly known as FLEX, and configure your clients to use the Barracuda NextGen Firewall F-Series as a proxy. The Barracuda Web Security Server is licensed on a per-user basis. If the number of users consistently exceeds the licensed number, traffic continues to be filtered, but you will be asked to upgrade your subscription to the actual user number. If the service expires, traffic is no longer filtered; it is only passed through.

Before You Begin

To configure the Barracuda Web Security service, you need the following components:

- A Barracuda Web Security subscription connected to your [Barracuda Cloud Control account](#).
- The serial number and proxy server host for your Barracuda Web Security service subscription:

To locate your serial number, log into your Barracuda Cloud Control account, and click on the **SUPPORT** tab in the **Web Security** section.



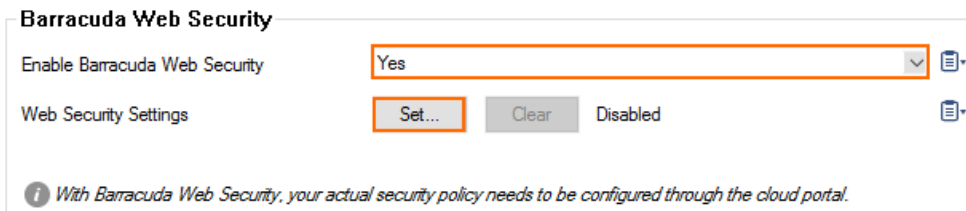
The screenshot shows the Barracuda Cloud Control interface. The top navigation bar includes 'Web Security' and 'SUPPORT' (highlighted). The left sidebar shows 'Web Security' selected. The main content area displays 'ACCOUNT INFORMATION' with the following details:

- Account ID: 100100
- Account Type: Barracuda Firewall Web Content Filtering Service
- Serial: 555555
- Subscription Expiration: 2014-12-16
- Service Host: ple1.proxy.purewire.com

Step 1. Configure the Barracuda Web Security Service

Enable the Barracuda Web Security service in the HTTP Proxy settings.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > HTTP Proxy > HTTP Proxy Settings**.
2. Click **Lock**.
3. Set **Enable Barracuda Web Security** to **Yes**.
4. Click **Set / Edit** to edit the **Web Security Settings**. The **Web Security Settings** window opens.



Barracuda Web Security

Enable Barracuda Web Security

Web Security Settings













With Barracuda Web Security, your actual security policy needs to be configured through the cloud portal.

5. Enter the **Web Security Settings** for your Barracuda Web Security service account:
 - **Web Security Service Host** - Enter the URL for your Barracuda Web Security service account. E.g., ple1.proxy.purewire.com
 - **Authentication Type** - Select **User/Password** to use your Barracuda Cloud Control credentials, or select **AuthenticationKey** to use an authentication key created in your [Barracuda Networks Account](#) on the **Web Security > Configuration > Key Management** page.
 - **Web Security Serial** - The Barracuda Web Security service serial number.
 - **Web Security User** - Your Barracuda Cloud Control username.
 - **Web Security Password** - (User/password authentication only) Your Barracuda Cloud Control password.

The password can consist of small and capital characters, numbers, and non alphanumeric symbols, except the hash sign (#).
 - **Web Security Key** - (Key authentication only) Select your authentication key.
 - **Use Web Security for SSL/TLS** - To redirect SSL/TLS HTTPS traffic to the Barracuda Web Security service, select **Yes**.

To also apply the Web Security Service policies to HTTPS traffic, you must create an [App Redirect](#) access rule that forwards HTTPS traffic to the local proxy IP address and port. There is no specific block error page. The end user receives a non-specific server error for blocked HTTPS pages.
 - **Excluded Domains** - Enter domains you do not want to forward for processing by the Barracuda Web Security service.

Web Security Settings

Web Security Service Host	<input type="text" value="ple1.proxy.purewire.com"/>		
Authentication Type	<input type="text" value="User/Password"/>		
Web Security Serial	<input type="text" value="555555"/>		
Web Security User	<input type="text" value="mmm@barracuda.com"/>		
Web Security Password	Current	<input type="text"/>	
	New	<input type="password" value="•••••"/>	
	Confirm	<input type="password" value="•••••"/>	
	Strength	<input type="text"/>	
Web Security Key	<input type="text"/>		
Use Barracuda Web Security for SS...	<input checked="" type="checkbox"/>		
Excluded Domains	<input type="text"/>	    	

6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Step 2. Configure your Clients to use Barracuda Web Security via the NextGen Firewall F-Series

Configure your clients to use the Barracuda NextGen Firewall F-Series as a forwarding proxy.

Figures

1. WSS.png
2. enable_web_security.png
3. set_web_security.png

© Barracuda Networks Inc., 2020 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.